10-05-2021

END-SEM

A.Sai Venkata Aditya

18BCS011

CS-360

1)
```
import os
def lamda- handler (event , ctext):

    a = "username1 "        d = "username3"
    b = "username2"

    c = input (" enter username")
    if (c == a)
     {    int k=1
          for i in range 1 to 10
            k=k+i
            return k;

     }
     else if (c== d)
           print (" Access")

           return

     else
        return error.
```

10-05-21

END

A·Aditya
18BCS011

2.) Java based building Lamda Functions

Lamda functions use an execution role to get permission to write logs to Amazon Cloud Watch logs

To create an execution role

⇒ Create role

⇒ Create role with following

Trusted entity - Lambda

Permissions - AWS Lambda Basic

Role name - lambda role

To create Java function

⇒ Open lambda console

⇒ Choose Create function

⇒ Name - my-function

Runtime - Java11

Role - choose an existing role

Existing role - lambda role

⇒ Create function

⇒ To configure test event choose Test

⇒ For Event name enter Test

⇒ Choose Create

⇒ To invoke the function choose Test.

To console create Lambda function with a handler class named Hello Since Java is a compiled Language. Java functions runtime gets invocation events from Lambda and passes them to handler. In the function configuration.

3) a) Cloud Watch, logs

b) ~~Cloud Watch Alarm~~ SNS

4) ⇒ To host a static website in AWS we are required to do following DNS restrictions

i) We know DNS helps to connect bucket and website we need to be careful and follow the restrictions as it is website endpoint

ii) IF we are hosting static website we need to link the data files present in S3 bucket to our website domain.

iii) If we don't follow then we are not able to give access and integrate S3 to our website domain which leads to us to an error 403 forbidden.

iv) Also it must not assessed by anyone so that it would not be accessed by any member.

v) Finally when we host a static website we are required to follow DNS restrictions as it is end point for a bucket.

Q5) Various modes of accessing the AWS cloud

AWS Console :- Easiest way to manage resources on AWS We can log in with the user you created above Lets copy the URL for the user login from the root acounts like

Since the user has only read-only access to the IAM you can't add a new user If you try to add you will get theerror S3 service and see all the buckets and create one This is a very easy process you can go ahead and do well with it.

AWS CLI :

It is a unified tool to manage your AWS services. With just one tool to download and configure you can control multiple AWS services from the command line and automate them through scripts

We need to configure our AWS CLI for the user we created above for that you should have access to the keys that you downloaded while creating the user and the command.

"

When you are done with the configuration we can use any service you have access to Create an S3 bucket and list all the buckets again with the settings we know

AWS SDK

AWS has tools for developing and managing applications on AWS. AWS supports these programming languages at time of writing C++. Create node.js project which is a RESET API to create buckets and list buckets Make sure we have security credentials Only two dependencies express & aws-sdk

AWS SDK allows us to programmatically manage services on AWS. AWS provides SDK for several programming Languages.

6) DDos Techniques to minimise this kind of attacks :-

i) Reduce Attack Surface Area :-

Mitigate DDos attack is to minimize the Surface area that can be attacked thereby limiting the options for attackers and allowing us to build protections in a single place

We want to ensure that we do not expose our application or resources to ports, protocols or applications from where they do not expect any communication

ii) Plan for scale :-

The two key considerations for ~~mig~~ mitigating large scale volumetoric DDos attacks are bandwidth capacity and server capacity to absorb and mitigate attacks.

Transit capacity: When architecting our applications Internet connectivity that allows us to handle volumes of traffic.

Server capacity:- Most DDos use up lot of resources It is important that you can quickly scale up resources

iii) What is normal and abnormal Traffic :

Whenever we detect elevated levels of traffic hitting a host the very baseline is to be able only accept as much as traffic as our host can handle without affecting availability. we need to understand the characteristics of good traffic that the target usually receives.

iv) Deploy Firewalls for Sophisticated Application Attacks

A due to the unique nature of these attacks you should be able to easily create customized mitigations aganist illegitimate requests which could have characteristics like disguising as good traffic or coming from bad IPs unexpected geographics.

Aditya
18BCS011

7) EC2 stop and EC2 Terminate both are actually different states in the AWS EC2 lifecycle

⇒ When we Stop EC2 Instances:-
It indicates that an instance is shut down and cannot be used. Basically it is a temporary shutdown for when you are not using an instance but the attached bootable EBS volume will be not deleted.
Ultimately the Instance store volumes data is erased when stopped. Even the RAM is erased when EC2 stopped.

⇒ When we Terminate EC2 Instances:-
On the other way It is permenent deletion Only Use this when you are finished with an instance as terminated instances cannot be recovered. The virtual machine that was provisioned to us will be permanently taken away and we will no longer be charged. Main point any data that was stored locally on the instance will be lost.

8) Following steps are used to recover access to your EC2 instance after when you lost instance login credentials.

1) Gather configuration details of the original (target) instance.

2) Power off the original (target) EC2 instance of which you want to regain access.

3) Launch new (recovery) instance and generate new key pair

4) Login via ssh terminal to the new recovery instance.

5) Detach the primary EBS volume from original (target) instance (taking note current attachment)

6) Attach /Mount the previously detached volume to the new (recovery) instance.

7) Copy authorized keys from recovery instance to the mounted (target) volume.

8) Unmount target volume from recovery instance and reattach back to original (target) instance using configs noted earlier

9) Start the original instance and login with new key-pair

10) Delete temporary instance.

THE END